# SAFETY IN NUMBERS

**Robert Filman** • Lockheed Martin • filman@mcc.com

"There is no safety in numbers, or in anything else." — James Thurber

This month the Spider explores what can go wrong when you hook your computer up to a network, what you can do about it, how you might go about making things go wrong, and what can go wrong when trying to deal with what can go wrong.

### WWW Security FAQ • www.w3.org/Security/Faq/

**Lincoln Stein**

The Spider's first stop is the World Wide Web Consortium's Security "Frequently Asked Questions" page. (Actually, it's more of a book than a page.)

Question 1 is, "What's to worry about?" If you've been blithely networking along, note that there are many possibilities.

- You thought you were making information available to the world, but you were actually providing a portal through which strangers can enter and manipulate your machine and its data. If you have different classes of users with different privileges, the problem compounds exponentially.
- You thought your Web-surfing safe and anonymous, but the ability of Web pages to run code opens a Pandora's box. Java attempts a sandbox model. At least security violations of the sandbox are bugs. In ActiveX, it's open season on anything and everything. There is no sandbox and no limit on active content. (The Spider recalls the ActiveX demo at Sun's JavaOne Conference a year and a half ago, where opening a Web page served to reformat the hard disk, write checks to deserving hackers, file an altered 1040 with the IRS, and shut down the machine. The author explained that he hadn't violated his ISP's antihacking rules, but was merely providing a way to remotely turn off a computer.) In any case, Web surfing isn't anonymous: sites accumulate data about visitors and cookie analysis can reveal patterns of use.
- And even if you've got a trustworthy user on a trustworthy machine, TCP/IP is an open, university-style protocol. Eavesdroppers are listening.

The FAQs cover topics such as running secure servers, keeping data secure, scripting, client-side security, alternative payment mechanisms, and particular products, and closes with a modest bibliography.

### Things that Go Bump in the Net • www.research.ibm.com/massive/bump.html

**David Chess, IBM**

A somewhat more metaphoric overview of what can go wrong can be found at this page, a small catalog of malicious programs. Can't tell a Trojan horse ("a program that does something that the programmer intended, but the user would not approve of if he knew about it in advance") from a worm ("a self-sufficient program that spreads by spawning copies of itself on other hosts in the network.") or a "Flying Dutchman" (a program that uses resources to benefit its creator, without compensation, that has become immortal) from a "Zombie" (a program that continues to use resources after it's been killed)? Check out this site. The list will likely suggest a few new exercises to fill your free time.

### Cryptography and Security • theory.lcs.mit.edu/~rivest/crypto-security.html

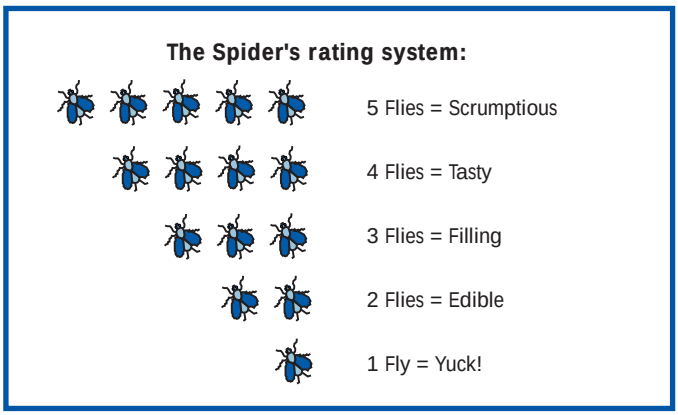
**Ron Rivest**

Probably the best set of pointers I've found to other security and cryptography pages is from one of the modern pioneers in digital cryptography, Ron Rivest. Links include bibliographies; government, nonprofit, university, and commercial organizations; news groups; alert sites; people; algorithms; software; and "other compilations of links."

### Infowar • www.infowar.com/

**Winn Schwartau**

Accelerate your security attacks and you too can wage an infowar, the subject of this site. Infowar gets high marks for content with a few demerits for organization. The site is presented in two frames, with sinister selections dexterously displayed. Choices include about two dozen topics such as privacy, espionage, terrorism, legal issues, products, resources, studies, tools, and news. Rather than being a source of original content, Infowar seems primarily to be links to a large number of news reports and articles. The Spider found news stories on current abuses, links to newsgroups and e-zines like Peter Neumann's *Risks* and the hacker journal *Phrack*, newspaper articles on the rising tide of ter-




rorism, and Chomsky on why Castro is entitled to bomb Washington (http://www.infowar.com/class_3/class3_082898b_j.shtml).

The Spider is impressed with the breadth and depth of material, and is even willing to tolerate the periodic advertisements for the author's services. I just wish the home page were a bit more descriptive of the site's overall goals and organization.

### *Phrack* Magazine • www.2600.com/phrack/

So, you ask, how can I too learn to hack network sites? I followed a link labeled "Where the elite meet to meet, greet, and stomp their feet" to a page describing successful hacks to the zine itself, with the suggestion that prospective electronic graffiti artists do their tagging there. Sort of in the spirit of CalTrans erecting a dummy overpass just for the taggers. A random sampling of articles combines the social (reports of meetings, with emphasis on the personalities involved) to technical discussions of system weaknesses (including code to exploit these weaknesses). Examples include a discussion of ways to redirect calls in shared libraries for "multiple purposes," a detailing of techniques to determine which ports of a host are active, and a simple method for bypassing checksum programs.

*Authentic, but a bit difficult to separate the wheat from the chaff.*

### AntiOnline • www.AntiOnline.com

If *Phrack* is the newsletter for hacking, AntiOnline is the graduate school. In contrast to *Phrack*, AntiOnline has a glossy appearance, complete with banner advertisements. (One of the advertisers is Microsoft, felicitous support given the opportunities their software provides.) AntiOnline contains archives of software, exploits, and news events, and a virtual library of hacking. For example, in the beginners section of the virtual library I found articles such as "Ethics of Hacking," "Hackers Encyclopedia" (common terms and famous people), "Hacking Kit" (hacking techniques), "Acquiring Account Information," and "Security Backdoors."

### DigiCrime • www.digicrime.com

**Kevin S. McCurley**

Not skilled enough to do your own hacking? Visit DigiCrime, which offers "a full range of criminal services and products to our customers." At DigiCrime I learned how to evade ITAR export cryptography restrictions (export your software by rocket), how to get free decryption cycles (use the applet cycles of your Web page visitors, as the site is happy to demonstrate), and how to collect password and bank account information (give people forms to fill out, once again as the site is pleased to illustrate). DigiCrime also includes a collection of examples of the security challenged, my favorite being Microsoft Bob. Bob evidently has the feature that a trice mistyped password is assumed to be forgotten. The system then offers to let the user set a new one. Or as the Microsoft product manager remarked, "It's not really an attempt at security." Right.

*Fun.*

### The Hacker Crackdown: Law and Disorder on the Electronic Frontier • www.lysator.liu.se/etexts/hacker/ (html) www.dcs.gla.ac.uk/SF-Archives/Bruce.Sterling/The.Hacker.Crackdown/ (plain text) secure.eff.org/pub/Publications/Bruce_Sterling/Hacker_Crackdown/ (all sorts of zipped formats)

**Bruce Sterling**

Well, with all these bad guys out to destroy the system, what are the defenders of truth, justice, and so on supposed to do? *The Hacker Crackdown* tells the story of the government's zeal in pursuing several people involved in the theft of a BellSouth document describing the administration of the 911 emergency response system.

"Knight Lightning" (Craig Neidorf, an editor of *Phrack*), was charged with the fraudulent interstate theft of property worth $79,449, his crime being publishing said document. Bruce Sterling was attracted to the case when the government seized the computer of a role-games publisher where one of the document thieves worked, contending their cyberpunk fiction was a real threat. Sterling, a cyberpunk science fiction writer, took this personally and investigated. He created an eminently readable description of the history of the phone system, phone system hacking, and the legal adventures of those caught up in this particular case. Sterling (rightfully) thought his book of sufficient import to the online community that he makes electronic copies freely available. (The online community has responded by copying it all over the place.) It's a great read. And as for Neidorf, the charges were dropped when the defense pointed out that AT&T would sell to anyone with a Visa card the same information for $13.